AMENDMENTS TO THE CLAIMS

Claim 1 (Currently Amended) A link lock system for a network, comprising:

a computer;

a network interface device to provide the computer with access to the network;

a bus monitor to monitor a first link between the network interface device and the computer, where the bus monitor reports detected failures or intrusions; and

a security switch to switch the first link from a non-secured mode using an HTTP protocol to a secured mode using an HTTP-S protocol when a report of the detected failures or intrusions is received from the bus monitor,

wherein data sent across the first link remains in the secured mode using the HTTP-S protocol when the report of the detected failures or intrusions is received from the bus monitor and is prevented from switching to the non-secured mode using the HTTP protocol until the detected failures or intrusions are corrected.

Claim 2 (Previously Presented) The system of claim 1, wherein the computer is a server.

Claim 3 (Previously Presented) The system of claim 1, wherein the network operates in the secured mode using the HTTP-S protocol.

Claims 4 -5 (Cancelled)

Claim 6 (Previously Presented) The system of claim 1, further comprising:

a controller that receives the report from the bus monitor and sends a control signal to the network interface device, the security switch, and the computer.

Claim 7 (Previously Presented) The system of claim 6, further comprising:

an encryption element in the computer, where the encryption element converts data placed on the first link using the secured mode when the control signal is received from the controller.

Claim 8 (Currently Amended) A system for a server, comprising:

an interface device to provide the server with access to a network; and

a controller to monitor a link between the interface device and the server, where the controller switches the link from a non-secured protocol using an HTTP protocol to a secured protocol using an HTTP-S protocol when failures or intrusions are detected on the link, wherein data sent across the link remains using the HTTP-S protocol when the failures or intrusions are detected and is prevented from switching to HTTP protocol until the detected failures or intrusions are corrected.

Claim 9 (Previously Presented) The system of claim 8, wherein the network is the Internet.

Claim 10 (Previously Presented) The system of claim 8, wherein the controller sends a control signal to the server when failures or intrusions are detected on the link.

Claim 11 (Previously Presented) The system of claim 10, further comprising:

an encryption element in the server, where the encryption element converts data placed on the link by the server using the secured protocol when the control signal is received from the controller.

Claim 12 (Currently Amended) A method, comprising:

monitoring a link between a network device and a computer;

first directing the link to use an HTTP-S protocol when failures or intrusions are detected on the link; and

second directing the link to revert to an HTTP protocol when the detected failures or intrusions have been corrected, wherein data sent across the link remains using the HTTP-S protocol when the failures or intrusions are detected and is prevented from switching to HTTP protocol until the detected failures or intrusions are corrected.

Claims 13-14 (Cancelled)

Claim 15 (Original) The method of claim 12, wherein the computer is a server.

Claim 16 (Currently Amended) An apparatus comprising a machine-readable storage medium having executable instructions that enable the machine to:

monitor a link between a network device and a server;

first directing the link to use an HTTP-S protocol when failures or intrusions are detected on the link; and

second directing the link to revert to an HTTP protocol when the detected failures or intrusions have been corrected,

wherein data sent across the link remains using the HTTP-S protocol when the failures or intrusions are detected and is prevented from switching to HTTP protocol until the detected failures or intrusions are corrected.

Claims 17-18 (Cancelled)

Claim 19 (Previously Presented) The method of claim 12, wherein the link reverts to the HTTP protocol when a network manager determines that the detected failures or intrusions have been corrected.

Claim 20 (Previously Presented) The apparatus of claim 16, wherein the link reverts to the HTTP protocol when a network manager determines that the detected failures or intrusions have been corrected.